PCT/EP01/00349 19/7

1765

BUNDESREPUBLIK DEUTSCHLAND

09/936303

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

EP 01 | 349

EJU

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	100 01 097.0
Anmeldetag:	13. Januar 2000
Anmelder/Inhaber:	SCM Microsystems GmbH, Pfaffenhofen an der Ilm/DE
Bezeichnung:	Elektronisches Zahlungssystem für Dienste, Software und multimediale Inhalte
IPC:	G 07 F, G 06 F, H 04 L

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 30. Januar 2001
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Waasmaier

Waasmaier

PRINZ & PARTNER GbR

PATENTANWÄLTE
EUROPEAN PATENT ATTORNEYS
EUROPEAN TRADEMARK ATTORNEYS

Manzingerweg 7
D-81241 München
Tel. +49 89 89 69 80

SCM Microsystems GmbH
Luitpoldstraße 6
85276 Pfaffenhofen

Unser Zeichen: S 4565 DE
HD

13.01.2000

ZUSAMMENFASSUNG

Elektronisches Zahlungssystem für Dienste, Software und multimediale Inhalte

Vorgestellt wird ein Zahlungssystem für diverse über Online bezogene Dienste oder Inhalte unter Verwendung einer Geldkarte. Die Bezahl-Transaktion erfolgt offline, so daß Engpässe vermieden werden, die bei Online-Transaktionen über einen Rückkanal zu befürchten sind.

PRINZ & PARTNER GbR

PATENTANWÄLTE
EUROPEAN PATENT ATTORNEYS
EUROPEAN TRADEMARK ATTORNEYS

Manzingerweg 7
D-81241 München
Tel. +49 89 89 69 80

SCM Microsystems GmbH
Luitpoldstraße 6
85276 Pfaffenhofen

Unser Zeichen: S 4565 DE
HD

13.01.2000

Elektronisches Zahlungssystem für Dienste, Software und multimediale Inhalte

Die Erfindung betrifft ein elektronisches Zahlungssystem für online, z.B. über das Internet oder andere Netzwerke, empfangene Dienste, Software oder multimediale Inhalte, insbesondere Bezahl-Fernsehen.

Das System wird wie folgt beschrieben:

SCM Microsystems , Pfaffenhofen January 11, 2000 (Confidential)
Patent application "Micro-Payments with E-Purse Cards on STB via Conditional Access modules"
The CAM/POS

Solutions on STBs (Set-Top-Box) are known for micro-payments for "Pay Per View", where the E-purse card is inserted instead of a subscriber card into the CAM (Conditional Access Module) on Request of an EPG (electronic program guide) or an specific event stimulated by a broadcast datastream (Video/Audio). The request for a (micro-)payment is prior to getting an entitlement for viewing a certain content, which will be unscrambled upon such payment initiated by the user. The exchange of the subscriber card is a requirement to allow for insertion of an e-purse card.

Payments with E-purse on STB are done today by setting up the interactive payment protocol of the STB including a CAM requesting for reading the e-purse card and communicating with a specific remote back-end server holding a merchant security card called P-SAM (Purchase Security Access Module), performing the secured financial transaction by interaction of the E-purse with a remote merchant card and storing the resulting transaction in a transaction storage inside the server. Upon such payment a pay per view can be de-scrambled by the CAM.

The disadvantage of such a solution with regard to the proposed invention is such, that a risk for congestion in the communication process with the merchant server could come across for example in a switched public telefone network, if a large quantity of viewers wanted to do such transactions at a certain time. The transactions would have to take place in a very short period, normally just before an event payable would be broadcast. Apart from the danger for the congestion, such a solution requires normally holding out resources for servicing many lines as well as holding out many merchant modules being capable of performing fast transactions simultaneously.

The invention proposes a better performing and more flexible solution with regard to the process for payment. The period of payment can be de-coupled from the pay-per-view event as proposed:

- to install the P-SAM inside a conditional access module (instead of in a remote server)
- to provide a method to locally secure transactions that they cannot be deleted/withheld for authorized collection (by fraudulent manipulations) by a service provider. The transmission of untransferred transactions would be initiated from the CAM.
- to establish a value storage in secured storage area where an prepaid amount/value is stored for enabling several smaller consecutive transactions for pay per views without the further interaction of the e-purse card. The subscriber card remains in the module as long as prepaid value is available.
- Allowing services by separate transaction recording in order to cope with a plurality of service providers
- to find a secure but open architecture to allow interaction of diverse conditional access systems with one or several e-purse systems or payment schemes

option:
to provide a solution to provide URL (Universal Remote Locator?) to Website and then make Payment/transfer payment alternately

The solution to propose would avoid congestion with limited server resources for lines.

Such architecture would provide :

An open STB communicating via a return channel path with back –end servers (services for clearing)
A Conditional Access Module incorporating:

- A standard filter /descrambler unit for filtering & descrambling standardized video/multimedia data-streams
- A smart card reader device function
- A merchant security module P-SAM (detachable)
- A transaction total value limitation storage
- A transaction storage
- A function for generation of displayable messages for support of payment procedures/user information or interaction
- Cryptographic coprocessing, verification of signatures (RSA algorithm)
- Secured memory
  - for storing session keys
  - holding signatures assigned to transactions, a group of transactions
  - having a stored value register for view per pulse functions
  - providing transaction log (with time stamping, if time broadcasted)
  - secured compartments holding transactions for multiple service providers
- A function to provide return path (modem) protocol support for remote communications with P-SAM, SmartCard and CAM functions
- A timer /clock calendar function

The steps for a payment are:
(For one time session payment)

1) the broadcaster sends a specific EMM (entitlement management maintenance) for single subscriber addressing with condition of prepaying a specific amount at a certain time broadcast, (optional for this purpose sending time and date). Setting timing conditions in the CAM

2) CAM filters a secret key from the broadcast stream (being send for a certain time),
   2a) may also come from the Smart card as a decrypted specific controlword or key,
   2b) stores the amount payable in the "hidden" RAM space (secure storage, space address belongs to a specific provider)
      2bb) filters a public-key for reading the certificate from the clearing house
   2c) ask user to confirm a specific payment for a single pay-per-view session
3) Check for limit in the "limit transaction storage" (CAM)
   3a) Get a session key from PSAM, authorizing the transaction,
   3b) get key signed with private key from subscriber card
   3c) store (session key) certificate in "secure storage"
      3cc) store session key on SmartCard
4) Ask for e-purse card insertion and for confirmation.
5) Cross-Check: Authentication of cards, PSAM-E-purse, verification of signatures (standard)
   5a) Initiate order request to user and get user decision
   5b) confirm by time stamping,
   5c) CAM initiates PSAM for transaction
6) Perform Transaction and store it in the CAM transaction storage
   6a) using controlword (derived from EMM)
      6aa)and generate an offset/secret address (with the help of the session key generated by the P-SAM)
   6b) generate time stamp (CAM) for session key from PSAM, signing it with public key from Content Provider
7) Enter subscriber card
   and after authorization to allow the standard descrambling process for pay per view
      7aa) comparison of session key in Smart Card, token for validation of transaction (if positive)

alternative:

7bb) make a comparison on a following broadcast request (another EMM) filtered and use this as token for validation of transaction (if positive)

8) Descrambling of Payload
(Start timer in CAM if pay per pulse)

9) Transfer of transactions,
9a) initiated (by call) from clearing service requesting for authentication, exchanging certificates
9aa) CAM verifies certificate from clearing house.
9 bb) sends the certificate from the Smart Card to the server, server returns the session key
9 cc) CAM allows access to transaction storage by session key
9b) transfer of transactions
9c) transfer initiated by CAM (when reloading e-purse), calling the server for reload

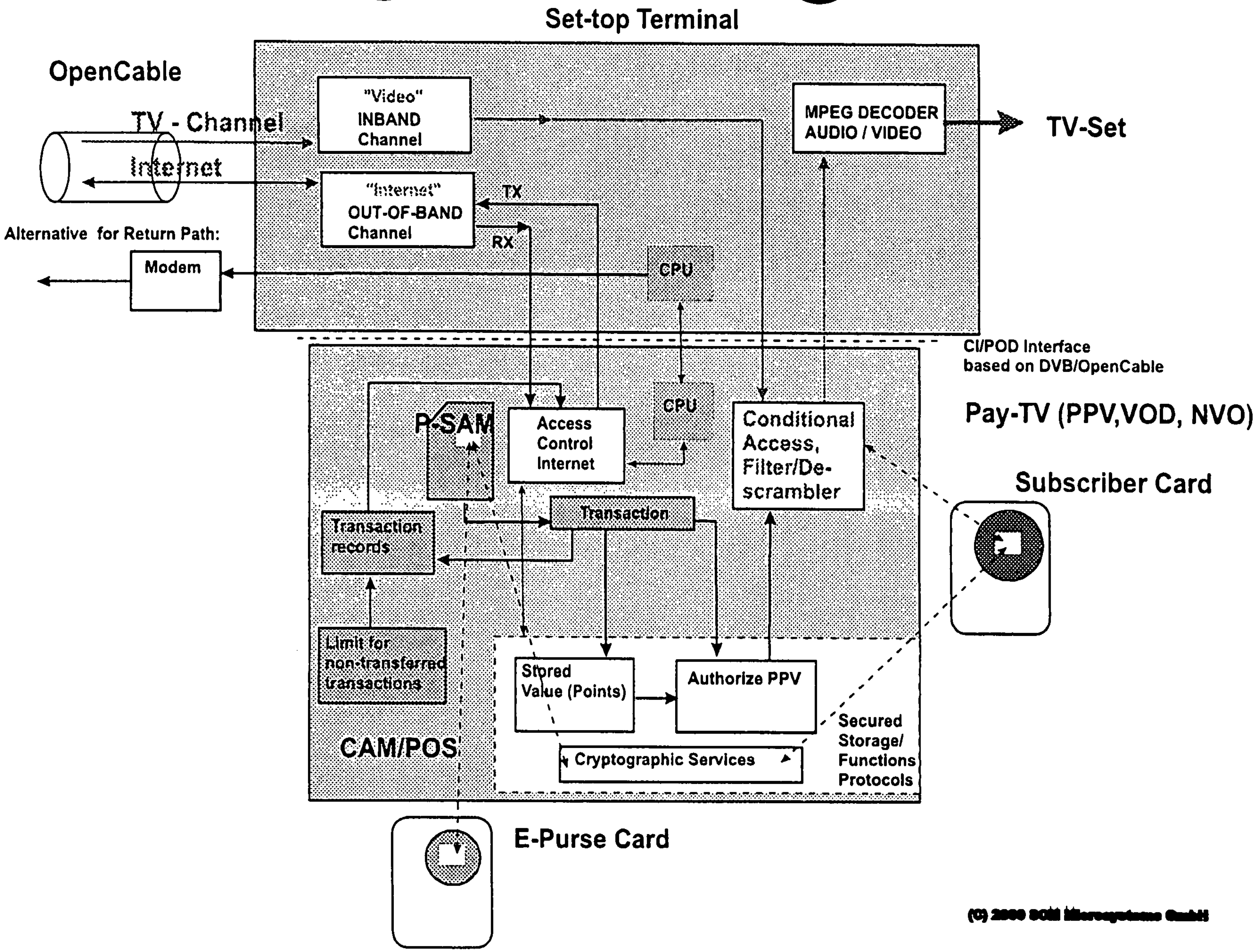
10) Records (journal) of transfers performed, sets status in the "limit transaction storage"

11) User initiated value transfer into e-purse (load)
11a) Sign session key and time with public key of content provider by Subscriber SmartCard

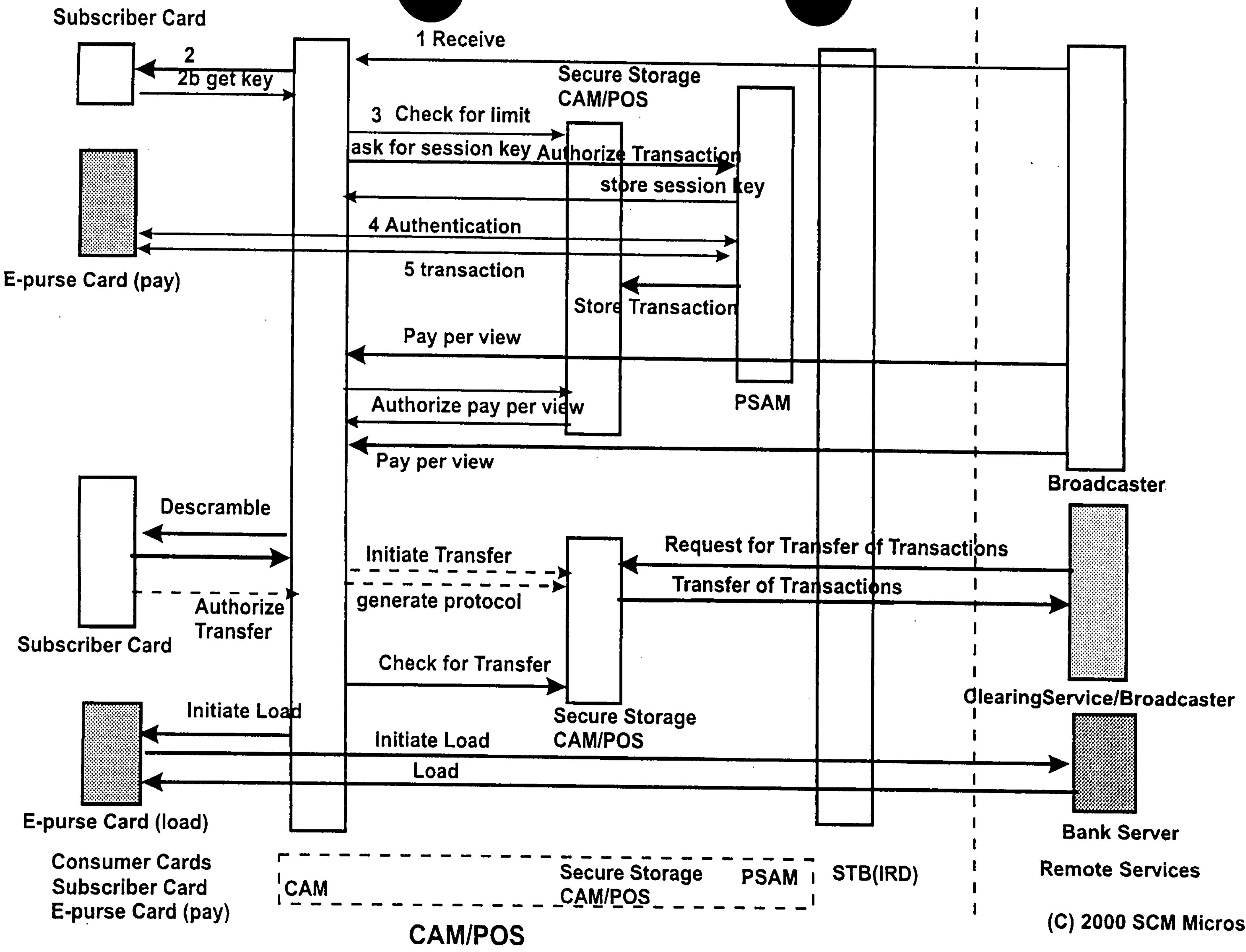
Prepaid Multiple session register

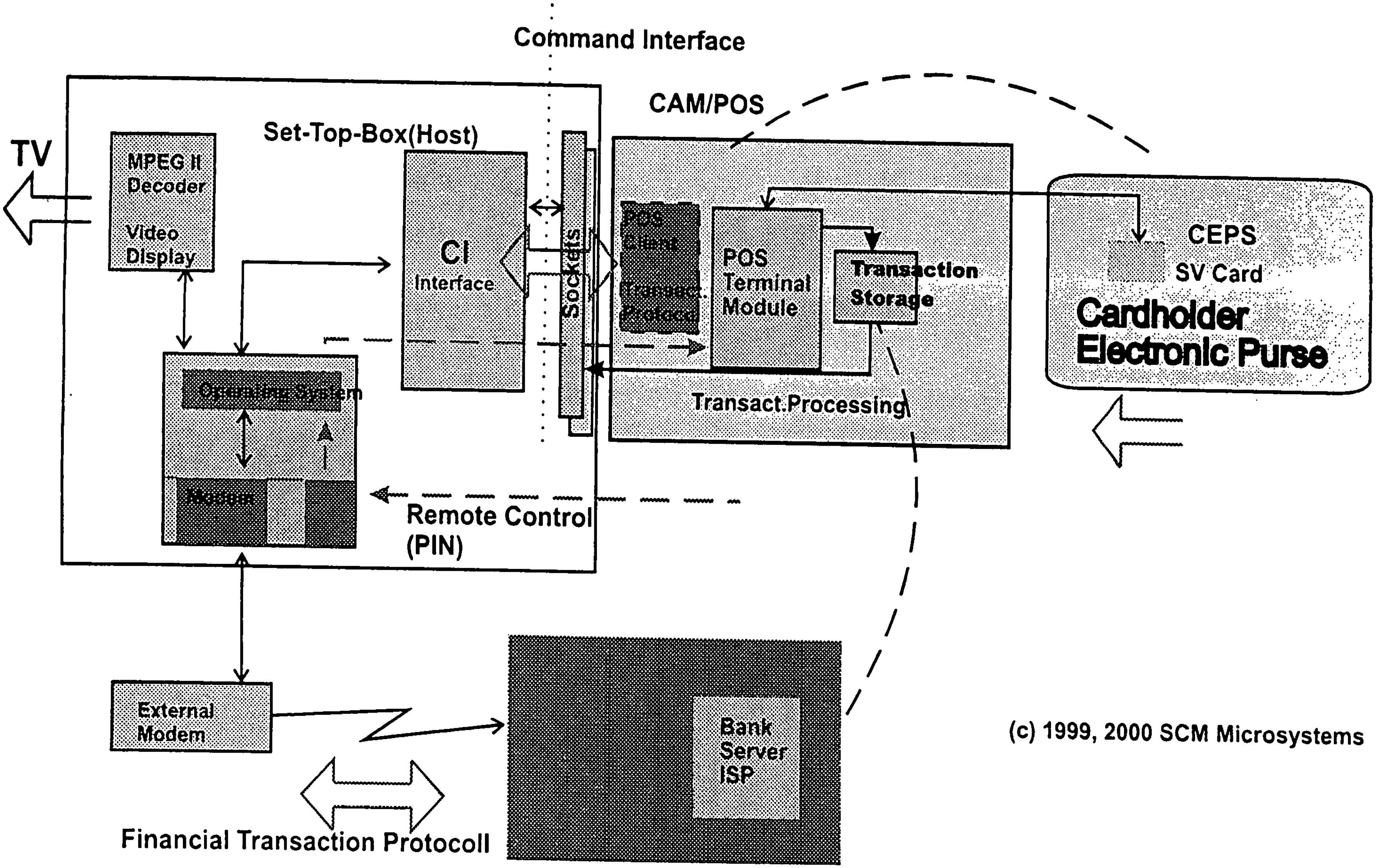
The basic payment is performed as defined above (1-7) however the payment is stored as value points in secured value register, from which value is deducted upon pay-per-view requirements. Value point transaction recording is done in a similar way. The transaction log is done under the same premises Another function is the deduction of smallest units equivalent to small micro-payments (1value point = 1 cent) for pay per pulse from the value register.

A specific value point transaction may allow to reconvert value points into e-cash and being restored on the e-purse card.

Set-top Terminal
OpenCable
TV - Channel
Internet
"Video" INBAND Channel
"Internet" OUT-OF-BAND Channel
TX
RX
MPEG DECODER AUDIO / VIDEO
TV-Set
Alternative for Return Path:
Modem
CPU
CI/POD Interface based on DVB/OpenCable
Pay-TV (PPV,VOD, NVO)
Subscriber Card
P-SAM
Access Control Internet
CPU
Conditional Access, Filter/De-scrambler
Transaction
Transaction records
Limit for non-transferred transactions
Stored Value (Points)
Authorize PPV
Cryptographic Services
Secured Storage/ Functions Protocols
CAM/POS
E-Purse Card

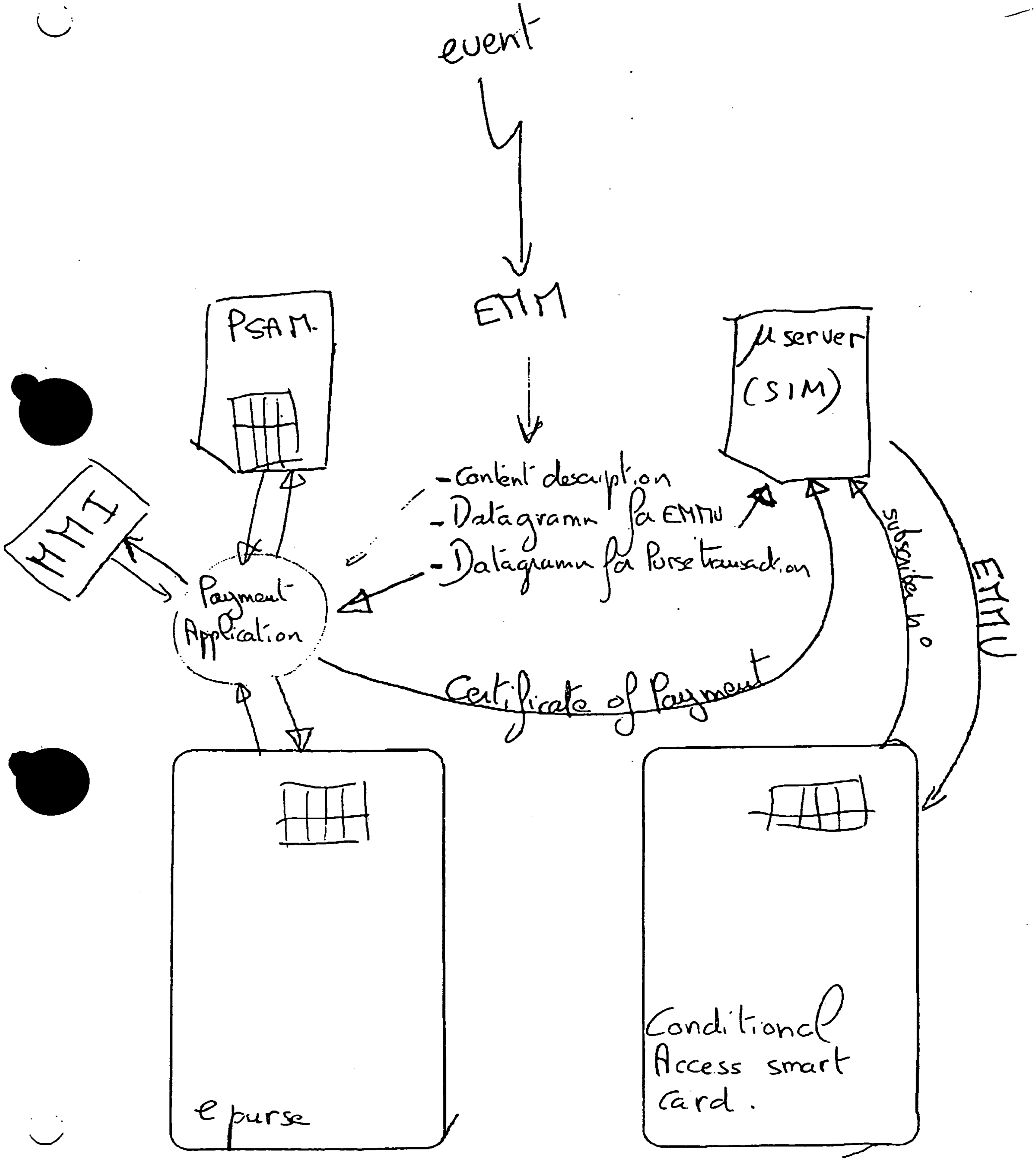
[illegible]enario I (single sessions pa[illegible]it)




Command Interface
CAM/POS
Set-Top-Box(Host)
TV
MPEG II Decoder
Video Display
CI
Interface
Sockets
POS Client
Transact. Protocol
POS Terminal Module
Transaction Storage
Transact.Processing
CEPS
SV Card
Cardholder Electronic Purse
Operating System
Modem
Remote Control (PIN)
External Modem
Bank Server ISP
Financial Transaction Protocoll

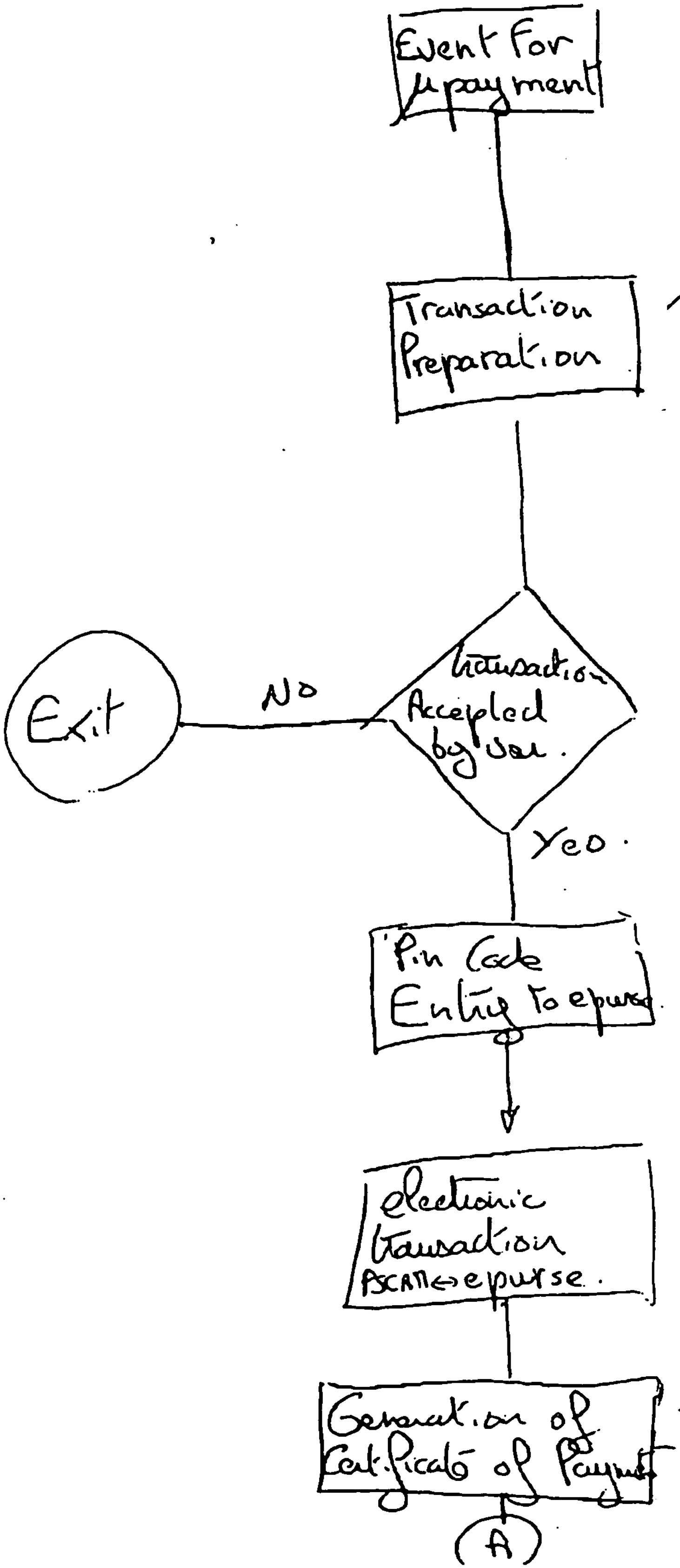
M 23.02.01

1/5


event
EMM
PSAM.
µ server
(SIM)
MMI
- Content description
- Datagramm for EMMU
- Datagramm for Purse transaction
Payment Application
Certificate of Payment
subscribe to
EMMU
e purse
Conditional Access smart card.

2/3

Transaction flow chart


Event for µpayment
Transaction Preparation
transaction Accepted by user.
NO
Exit
Yes.
Pin Code Entry to epurse
electronic transaction PSCAM↔epurse.
Generation of Certificate of Payment
A

→ by using content description parameters, Appli is using screen and remote control To set The transaction with USER ....

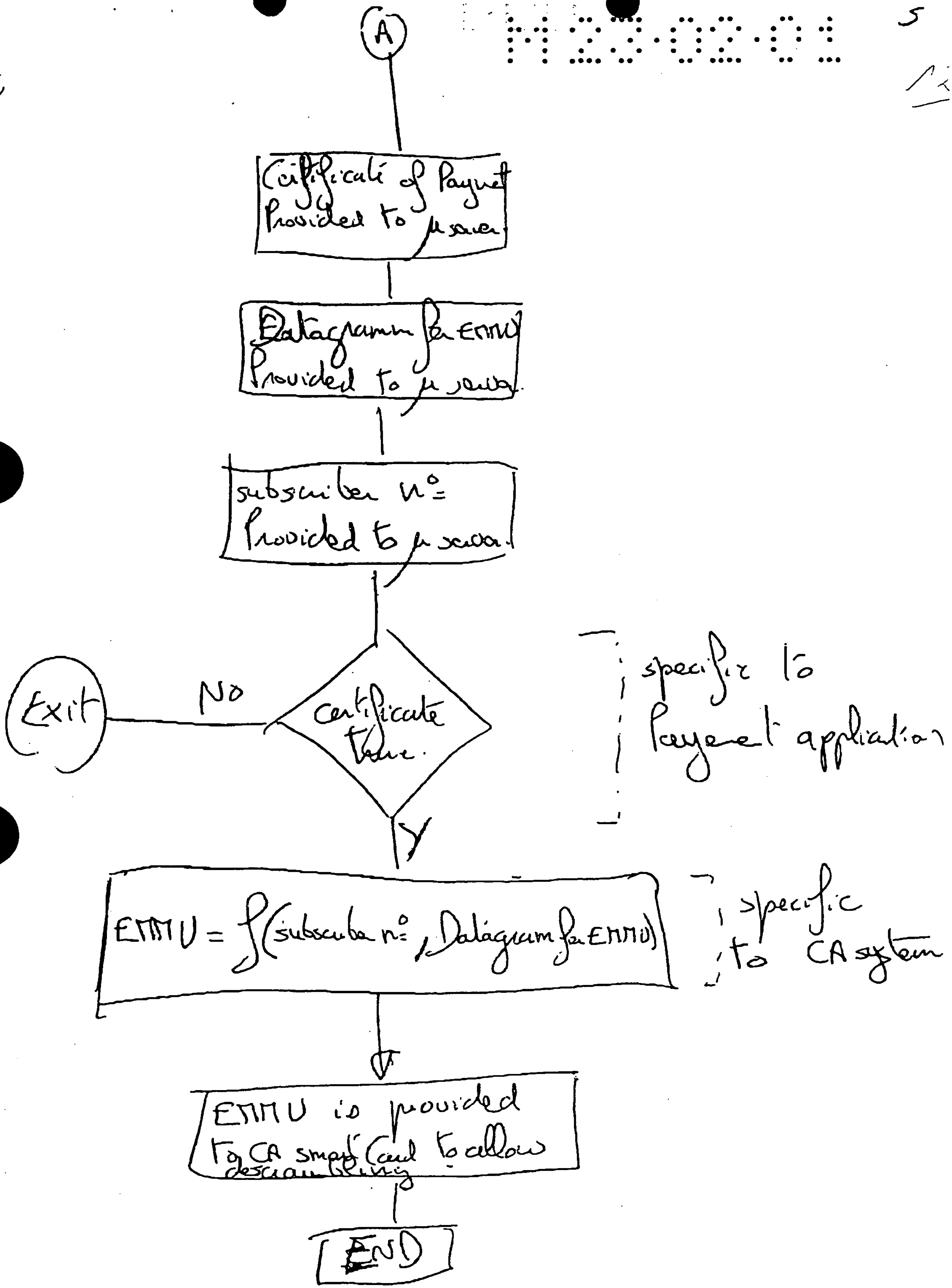
→ optional.

→ using "Datagramm for Purse transaction" as input.

→ certificate of Payment is stored in a safe way for further download

M 23.02.01

3/5


A
Certificate of Payment Provided to μ saver.
Datagramm for EMMU Provided to μ saver.
subscriber n°= Provided to μ saver.
certificate true.
No
Exit
Y
specific to Payment application
EMMU = f(subscriber n°, Datagram for EMMU)
specific to CA system
EMMU is provided to CA smart Card to allow descrambling
END

(+) µ server can be :

- specific module.
- Applet Loaded in PSCAM
- Applet Loaded in epurse.
- Applet Loaded in CA smart Card -

(+) When this system is used with a satellite receiver for data broadcast, to receive files on a PC, ~~B~~ we can provide more than payment/acces control feature, all the parameters used by the µ server :

- Datagramm for EMMU.
- ~~Datagramm for~~
- Certificate of Payment
- Subscriber number
- EMMU.

Can be USED AS A LICENCE NUMBER.

If the download system on the PC is done in a way to collect those informations and to append them in the file, the file will received the ~~certificate~~ licence number: means

5/5

illegal copy can be detected.

~~It's a kind of water marking~~

PSAM: Purchase Secure Access Module.

EMM: Entitlement Management Message.

MMI. Man Machine Interface.

epurse: electronic Purse.

EMMU: EntitlemenManagement Message Unique.

PRINZ & PARTNER GbR

PATENTANWÄLTE
EUROPEAN PATENT ATTORNEYS
EUROPEAN TRADEMARK ATTORNEYS

Manzingerweg 7
D-81241 München
Tel. +49 89 89 69 80

SCM Microsystems GmbH
Luitpoldstraße 6
85276 Pfaffenhofen

Unser Zeichen: S 4565 DE
HD

13.01.2000

Patentansprüche

1. Elektronisches Zahlungssystem für Dienste, Software und multimediale Inhalte, die Online bezogen werden, unter Verwendung einer Geldkarte, wobei die Bezahlungs-Transaktion Offline gemäß in einem geschützten Speicherbereich abgelegten Prozeduren erfolgt.

2. System nach Anspruch 1, bei dem eine Händler-Kartenfunktion durch Software in geschützten Speicherbereichen nachgebildet wird.